## REMARKS

Reconsideration of the pending application is respectfully requested on the basis of the following particulars:

Rejection of claims 1-26 under 35 U.S.C. § 103(a)

Claims 1-3, 5-7, 10-21, and 23-26 presently stand rejected as being unpatentable over Buffam (U.S. 6,185,316) in view of Vafai et al. (U.S. 6,279,133), and claims 4, 8, and 9 are rejected as being unpatentable over Epstein and Vafai and further in view of Camp, Jr. et al (U.S. 6,075,987). This rejection is respectfully traversed for at least the following reasons.

It is respectfully submitted that Buffam and Vafai, either individually or in combination, fail to form a prima facie case of obviousness of the presently claimed invention because these references, taken together, fail to disclose or suggest all of the claim limitations of independent claims 1 and 20, and because there is no motivation or suggestion for any combination or modification of these references to arrive at the presently claimed invention.

Neither Buffam nor Vafai disclose or suggest decrypting an encrypted code word on the basis of a digitized biometric authentication feature data thereby obtaining a decrypted code word, and recovering secret data from the decrypted code word on the basis of a coding-theory method within a freely selectable tolerance level.

Buffam does not disclose or suggest fault-tolerantly coding/decoding of secret data, as the examiner acknowledges in the recent Office action (at page 3).

While the examiner states that Buffam discloses that "secret data is recovered from the decrypted code word on the basis of a coding theory method **within a freely selectable tolerance level** (col. 22, lines 16-36)" (emphasis added by the examiner), Applicant respectfully disagrees.

The passage referenced by the examiner begins with the statement that "because ***pattern matching is fundamental*** to the operation of any biometric system, it can be

considered to be a primary factor when evaluating a specific biometric product. Thus, an acceptable biometric authentication system is accurate, relatively simple to deploy, and having a selectable tolerance adaptable to a variety of pragmatic factors" (Buffam; col. 22, lines 16-21) (emphasis added).

Buffam continues, stating that "the flexibility provided by features of this invention can be particularly advantageous in biometric implementations, where an adjustable ***matching error tolerance*** can be an important factor in tailoring authentication system performance to IT system needs" (Buffam; col. 22, lines 22-26)(emphasis added).

Buffam's reference to a ***matching error tolerance*** in a ***pattern matching*** function is not, and cannot be construed to be, the same as or similar to recovering secret data from a decrypted code word on the ***basis of a coding theory method*** within a freely selectable tolerance level.

This is underscored by the examiner's statement that "Buffam does not teach fault-tolerantly coding/decoding the secret data," at page 3 of the recent Office action.

Since Buffam does not teach or suggest such a coding or decoding of a secret data, then it necessarily follows that Buffam's error tolerance is not related to any such coding/decoding.

Buffam's matching error tolerance is simply a degree of difference, between a pattern template and a pattern sample, which is acceptable to declare that the sample matches the template notwithstanding some difference.

This has no relationship to (and in fact avoids entirely) any notion of "***correcting***" the sample, or "decoding" the sample according to recover secret data from a decrypted code word on the ***basis of a coding theory method*** within a freely selectable tolerance level.

The examiner asserts that "it would have been obvious [...] to combine fault-tolerant coding the secret data, as taught by Vafai et al., with the apparatus of Buffam," and further states that "it would have been obvious for such modifications because fault-

tolerantly coding data is widely in use for correcting data from disk drives and other storage," and because "correct data is needed to compare to a biometric sample."

However, it must be noted that, while fault-tolerant coding is widely in use for correcting data from disk drives and other storage, the present invention (and that of Buffam) deals with evaluation of a biometric sample, and not with insuring correct data is written to or read from a disk drive.

The examiner's statement that "correct data is needed to compare to a biometric sample" appears to mischaracterize both the present invention and Buffam.

Buffam provides no teaching or suggestion of any necessity to correct a biometric sample, which is to be compared to a template for validation. On the contrary, while Buffam does allow some tolerance in comparing the sample to the template, no correction of the sample is taught or suggested. Instead, any value that is not declared to be a match is simply deemed not authenticated (see Buffam; col. 22, lines 16-37).

Following the examiner's statement, one would apply the teachings of Vafai to the Buffam's reading of template data from a smart card. However, Buffam does not apply any selectable tolerance to the data read from the smart card, so there can be no teaching or suggestion according to this combination of decrypting an encrypted code word on the basis of a digitized biometric authentication feature data thereby obtaining a decrypted code word, and recovering secret data from the decrypted code word on the basis of a coding-theory method within a freely selectable tolerance level.

Conversely, the examiner has not stated any motivation or suggestion to apply a coding-theory method to the biometric sample itself, rather than the stored template, and the references themselves to not provide any such motivation or suggestion.

Notwithstanding that Buffam allows for a tolerance in pattern matching to determine an authentic biometric sample, nothing in Buffam suggests that a biometric sample can be construed to comprise a ***correctable error***. Instead, a mismatch between a proffered image (biometric sample) and the template is a valid condition, resulting in denied access.

Applicant notes that this is similar to the deficiency of the Epstein reference cited in previous Office actions, and discussed in Applicant's previous responses, except that Buffam allows for a less-than-exact match. As pointed out with respect to Epstein, any correction of a mismatching entered biometric key would defeat the purpose of Epstein's biometric identification mechanism, since invalid entered biometric key data could result in access being incorrectly granted.

***Tolerance*** of a less-than-exact match, such as is allowed by Buffam, is different from, and cannot be construed to be, a ***correction*** of error within a selectable tolerance interval. Nothing in Buffam suggests that it is desirable or useful to correct any mismatch. Further, nothing in Buffam suggests that a sample that is a less-than-exact but tolerable match is correctable, or that any benefit could be obtained by such a correction. Correction of data outside of the tolerance range would result in incorrect authentication, and correction of data inside the tolerance range is pointless, since by its very nature, Buffam treats data within the tolerance range as "valid" or matching.

On the other hand, Vafai is concerned with finding and correcting as may errors as possible. Accordingly, it is counter to the teachings of Vafai to provide a tolerance wherein errors are simply accepted and not corrected. Moreover, it is entirely counter to the teachings of Vafai to discard data which is read without any errors, while this is permitted in the present invention if the tolerance interval is set to exclude an exact match.

According to the present invention, if a number of deviations of a biometric feature detected during an authentication phase is within a predetermined number of deviations of a representation of the biometric feature determined during an initialization phase, then the biometric feature of the authentication phase is corrected and the corrected biometric feature used for restoring a secret key of the public key process, provided that the number of deviations detected in the authentication phase are within the tolerance range.

If the number of deviations detected in the authentication phase are not within the tolerance range (either too may or too few), then the biometric feature detected during the authentication phase is rejected. Any biometric feature detected in the authentication

phase and exactly corresponding to that of the initialization phase (having no deviations) may be rejected as falling outside the tolerance interval, making "replay attacks" difficult.

Because Buffam and Vafai fail to teach or suggest all of the claim limitations of independent claims 1 and 20, and because there is no motivation or suggestion for the combination of Buffam and Vafai as set forth in the recent Office Action, these references fail to form a prima facie basis of obviousness of any of claims 1-26. Accordingly, for at least these reasons, withdrawal of these rejections is respectfully requested.

Conclusion

In view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. Accordingly, it is requested that claims 1-26 be allowed and the application be passed to issue.

If any issues remain that may be resolved by a telephone or facsimile communication with the Applicant's attorney, the Examiner is invited to contact the undersigned at the numbers shown.

Respectfully submitted,

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314-1176
Phone: (703) 683-0500

Date: February 23, 2007

JOHN R. SCHAEFER
Attorney for Applicant
Registration No. 47,921